



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/510,284

11/09/2005

Christophe Giraud

0579-1071

7544

466

7590

11/27/2009

YOUNG & THOMPSON

209 Madison Street

Suite 500

Alexandria, VA 22314

EXAMINER

REVAK, CHRISTOPHER A

ART UNIT

PAPER NUMBER

2431

NOTIFICATION DATE

DELIVERY MODE

11/27/2009

ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

DocketingDept@young-thompson.com

<b>Office Action Summary</b>	<b>Application No.</b> 10/510,284	<b>Applicant(s)</b> GIRAUD, CHRISTOPHE	
	<b>Examiner</b> Christopher A. Revak	<b>Art Unit</b> 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 13 July 2009.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-9 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-9 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 06 October 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some \*    c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>11/2/09</u> . | 6) <input type="checkbox"/> Other: _____  |

## **DETAILED ACTION**

### ***Response to Arguments***

1. The applicant's amendments to the specification and claims have overcome the objections and rejections under 35 USC 101 and 35 USC 112 2<sup>nd</sup> paragraph.
2. Applicant's arguments filed with respect to the rejections of claims 1-9 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new grounds of rejection is made in view of Shimizu.

### ***Information Disclosure Statement***

3. The information disclosure statement (IDS) submitted on November 2, 2009 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

### ***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Art Unit: 2431

5. Claims 1-5,7, and 8 are rejected under 35 U.S.C. 102(b) as being anticipated by Shimizu, JP 10-154976. The citations are based on a machine translation of the teachings.

As per claim 1, it is taught of a method of making an electronic entity with encrypted access secure when said electronic entity executing a cryptographic algorithm consisting in applying to an input message a succession of groups of operations known as "rounds" involving a series of respective sub-keys produced successively by an iterative process starting from an initial key K, the method comprises performing steps of said iterative process so as to obtain a result of an iterative step, storing in said electronic entity said result of said intermediate step, repeating at least some of the steps of said iterative process until a result is recalculated corresponding to the result that has been stored, comparing the value of said stored result to the value of the corresponding recalculated result, and prohibiting the broadcasting of an encrypted message resulting from the application of said algorithm if said two values are different (see page 2, paragraph 70 through page 4, paragraph 73).

As per claim 2, it is disclosed of a method according to claim 1, further comprising storing a sub-key and repeating at least some of the steps of said iterative process until a sub-key is recalculated corresponding to said stored sub-key (see page 2, paragraph 70 through page 4, paragraph 73).

As per claim 3, it is taught of a method according to claim 1, further comprising storing the value of an intermediate result (R.sub.m) of said iterative process and repeating at least a portion of said iterative process until an intermediate result is

recalculated corresponding to the stored intermediate result (see page 2, paragraph 70 through page 4, paragraph 73).

As per claim 4, it is disclosed of a method according to claim 2, further comprising storing the value of the final sub-key (K.sub.n) and repeating at least a final portion of the steps of producing the succession of said sub-keys until said final sub-key is calculated a second time (see page 2, paragraph 70 through page 4, paragraph 73).

As per claim 5, it is taught of a method according to claim 4, further comprising repeating all of the steps of producing the succession of said sub-keys (see page 2, paragraph 70 through page 4, paragraph 73).

As per claim 7, it is taught of a method according to claim 1, wherein the method applied to a DES algorithm (see page 2, paragraph 70).

As per claim 8, it is disclosed of an autonomous electronic entity wherein it comprises means for implementing the method according to claim 1 (see page 2, paragraph 70 through page 4, paragraph 73).

### ***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2431

7. Claims 6 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shimizu, JP 10-154976. The citations are based on a machine translation of the teachings.

As per claim 6, the teachings of Shimizu fail to disclose of the use of AES. The examiner hereby asserts that it would have been obvious to apply the use of AES to the teachings of Shimizu. It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply an alternative means of encryption to the teachings of Shimizu so that the teachings were not limited to be used solely with the DES algorithm. According to the Supreme Court, the teaching, suggestion, or motivation test (TSM test) is one of a number of valid rationales that could be used to determine obviousness. It is not the only rationale that may be relied upon to support a conclusion of obviousness. (*KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385 (2007)). The claim would have been obvious because the substitution of one known element for another (AES algorithm for the DES algorithm) would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

As per claim 9, the teachings of Shimizu disclose of an encryption circuit (see page 3, paragraph 71), but fail to disclose of implementing the teachings through use of a microcircuit card. It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply an alternative means of a processing device to the teachings of Shimizu. According to the Supreme Court, the teaching, suggestion, or motivation test (TSM test) is one of a number of valid rationales that could be used to determine obviousness. It is not the only rationale that may be

Art Unit: 2431

relied upon to support a conclusion of obviousness. (*KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385 (2007)). The claim would have been obvious because the substitution of one known element for another would have yielded predictable results to one of ordinary skill in the art at the time of the invention. The teachings of Shimizu disclose of using encryption circuitry and any suitable device with processing means, such as a microcircuit card, could be used to carry out the teachings of Shimizu.

### ***Conclusion***

8. Applicant's submission of an information disclosure statement under 37 CFR 1.97(c) with the fee set forth in 37 CFR 1.17(p) on November 2, 2009 prompted the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 609.04(b). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Thursday, 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 517-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher A. Revak/  
Primary Examiner, Art Unit 2431